CCPA vs GDPR
A substantive comparison

Dr Gabriela Zanfir-Fortuna

June 24, 2019

Tel Aviv

FUTURE OF PRIVACY FORUM

Plan

1) Taking "the identical" out of the way
2) Three biggest differences
3) Three biggest similarities
4) Comparative galore:
   - ✓ Scope of application: to what, to whom and where does it apply?
   - ✓ Privacy Notice
   - ✓ Rights of the individuals
   - ✓ Service Providers/Processors
   - ✓ Security obligations

FUTURE OF PRIVACY FORUM

1) Taking "the identical" out of the way

Some wording from the GDPR has been transplanted to the CCPA

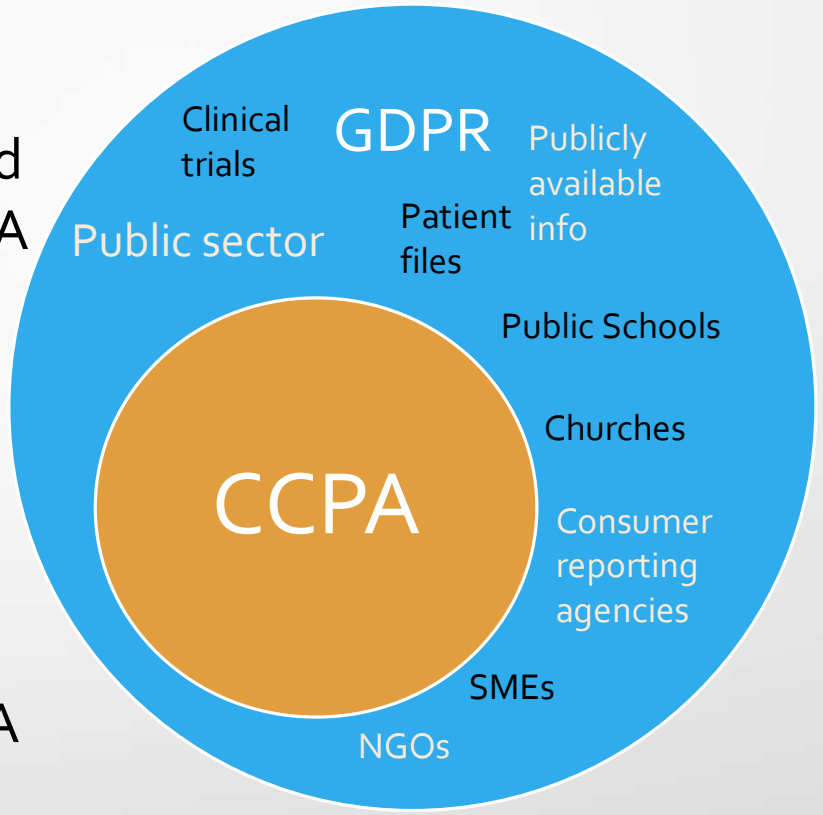
- Definition of 'pseudonymization' [Sec. 1798.140(r)]
- Definition of 'business' (controller) [Sec. 1798.140(c)(1)]
- References to 'portable' and 'readily usable format' [Sec. 1798.100(d)]
- Definition of 'processing' [Sec. 1798.140(q)]
- The concept that personal information can be any information, including information that can be 'reasonably linked, directly or indirectly', to a person [Sec. 1798.140(o)]
- The concept of 'compatible purposes' [Sec. 1798.140(s)(1)]
- An exception for 'scientific, historical or statistical research' for erasure [Sec. 1798.05(6)]

FUTURE OF PRIVACY FORUM

2) Three biggest differences

1 -> Scope: The GDPR applies to **everything** except for law enforcement, national security and purely personal activities, the CCPA applies to the **private sector only** and it excludes:

- SMEs or businesses that don't meet the threshold
- Nonprofits (schools, NGOs, churches etc.)
- Data regulated by HIPAA, GLBA
- Credit reporting agencies
- Publicly available information
  * Employment relationships (?)



FUTURE OF PRIVACY FORUM

2 -> Lawful grounds for processing: The CCPA **does not limit collection of personal data, at all.**

What does this mean in practice?

- No need for lawful grounds of processing, such as consent, legitimate interests etc.
- No purpose specification or data minimization requirements (business only have the obligation to disclose the purpose for which they collected personal information in the notice, but the purpose doesn't have to be specific, explicit and it does not count for obtaining consent or otherwise justifying the collection, nor for assessing minimization).

FUTURE OF PRIVACY FORUM

3 -> Private right of action: The GDPR has a complex system of remedies in place, including **a private right of action for any infringement of the law**, irrespective of whether damage was caused or not, as well as a private right of action to ask for any damages, material or immaterial (moral).

The CCPA provides for a limited private right of action:

- It only applies to data breaches of data that was not encrypted or de-identified;
- And it is contingent to a 30 days cure period.

FUTURE OF PRIVACY FORUM

2) Three biggest similarities

1) -> The definition of personal information/personal data

CCPA – "personal information"	GDPR – "personal data"
information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household *Includes a list of specific examples, including* - *(online) identifiers,* - *geolocation* - *biometric data,* - *Internet or other electronic network information and…* - *olfactory information (!)*	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

FUTURE OF PRIVACY FORUM

2 -> Individual rights that aim at giving some control over one's own personal data.

CCPA	GDPR
Right to request disclosure from businesses that collect PI and businesses that sell PI	Right of access (i.e. obtaining confirmation that PD are being processed)
Right to obtain specific pieces of PI	Right of access (i.e. obtaining a copy of PD)
Right to obtain pieces of PI in a portable format	Right to data portability
Right to request deletion	Right of erasure/to be forgotten
Right to opt out from selling PI	Right to withdraw consent, right to object
Notice to consumers	Right of information
Right to equal service and price	Partial overlap – freely given consent

FUTURE OF PRIVACY FORUM

3 -> Fines and supervisory authority

CCPA	GDPR
• Appointed authority: Attorney General of California • Sanctions: civil penalties up to 7500 USD for each intentional violation and 2500 USD for each non-intentional violation	• Appointed (&dedicated) authority: specialized Supervisory Authorities for data protection law + European Data Protection Board • Sanctions: two tiers – (1) up to 10 mil EUR or 2% of Global Annual Turnover; (2) up to 20 mil EUR or 4% of Global Annual Turnover.

Example:

A business creating and operating a mobile app for selling fashion items is found to:

- Not provide opt-out link for selling preferences of its users to its commercial partners (1 violation)
- For all its 10.000 users (10.000 x 1 violation = 10.000 violations x 7500$; Maximum fine can go up to 75,000,000$)

FUTURE OF PRIVACY FORUM

4) In depth comparison

Scope of application

CCPA: Sharing; Selling; Collection; Processing (?) [But different rules apply to different operations]	GDPR: Processing [all rules apply to processing PD]
Collection: buying, renting, gathering, obtaining, receiving, or **accessing** any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior **Selling:** includes renting, disclosing, releasing, disseminating, making available, transferring, or otherwise communicating personal information for monetary or 'other valuable consideration'	Any operation performed on personal data 'such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'

FUTURE OF PRIVACY FORUM

Consumers	Data subjects
a natural person who is a California resident	a living natural person who is physically in the EU or whose PD are processed by an entity established in the EU
Businesses	**Controllers and Processors**
(1) collect consumers' personal information, or on the behalf of which such information is collected + (2) alone, or jointly with others, determines the purposes and means of the processing (3) that does business in the State of California, and (4) meets certain threshold requirements (annual gross revenue exceeds $25m; annually sells the PI of > 50,000 or derives > 50% of its annual revenues from selling PI; and any entity that controls or is controlled by such a business.	**Controllers**: organizations (private and public) and persons who establish the means and purposes of processing **Processors**: entities that process PD on behalf of Controllers Territorial conditions: C & P must either be established in the EU, or provide goods, services to or monitor the behavior of persons in the EU

FUTURE OF PRIVACY FORUM

Notices/Right of information

CCPA: Privacy Policy (whenever PI is collected)	GDPR: Notice to be provided
Include in existing privacy policies or create a new one with the following details: • Description of rights and at least one method to exercise them • A list of categories of PI collected • A list of categories of PI that were sold in the previous 12 months, or the fact that PI was not sold • A list of categories of PI that were disclosed for a business purpose in the previous 12 months • A link to 'Do Not Sell My Personal Information' **To be updated every 12 months!**	In a clear language and must be readily accessible. Provide details about: • the identity of the controller • lawful grounds for processing used • contact details including those of the DPO • purposes of processing • intention to transfer data outside the EU • data retention period • existence of rights • existence of ADM including profiling and the logic involved therein • whether the provision of data is a statutory or contractual requirement • sources of data, if collected indirectly

FUTURE OF PRIVACY FORUM

Right of access

CCPA: Applies to PI that has been 'collected' or 'sold'	GDPR: Applies to PD that is being 'processed'
• Categories of PI it has collected/sold about that consumer • The categories of sources from which the PI is collected • The business or commercial purpose for collecting/selling PI • The categories of third parties with whom the business shares PI • Existence of deletion right	• Purposes of processing • Categories of PD processed • Retention periods • Sources of PD • Existence of other rights, including to complain • Existence of profiling, automated decision-making (ADM) • Logic involved in profiling, ADM
• The 'specific pieces of PI it has collected' about that consumer.	• A copy of the PD that are processed
• Reply in 45 days, that can be extended once (justified) • Free of charge	• Reply in 30 days, which can be extended (justified) • Free of charge, unless excessive request

FUTURE OF PRIVACY FORUM

Portability

CCPA: Portability follows the right of access: when businesses provide data electronically to the consumer, it should be sent in a 'portable and readily usable format that allows for the transmission of this information to another entity without hindrance'	GDPR: Right to receive personal data processed on the basis of contract or consent in a 'structured, commonly used, and machine-readable format' and to transmit that data to another controller 'without hindrance'.
Applies to all personal information subject to the right of access (e.g. including inferences)	Applies only to personal data provided to the controller by the data subject (it excludes inferences)
Includes only business to consumer transmission of PI	Includes controller to controller transmission of data

FUTURE OF PRIVACY FORUM

Right to deletion/erasure

CCPA: Applies to PI that has been 'collected'	GDPR: Applies to PD that is being 'processed'
A consumer can request deletion in all circumstances, unless exceptions apply	A data subject can request erasure in certain circumstances only – PD are no longer necessary to achieve the purpose, unlawful processing, withdrawal of consent, successful objection.
Exceptions, where PI is needed to/for: • Complete a contract or provide a service/good requested by the consumer • Detect security incidents • Free speech • Comply with other California laws • Scientific, historical, statistical research (et al, 9 in total)	Exceptions: • Freedom of expression • Legal obligation • Public health • Archiving or scientific, historical, statistical research • Establishment, exercise or defense of legal claims

Right to opt-out/object

Selling of PI	Processing of PD
• right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's PI	• Withdrawal of consent • Right to object to direct marketing • Right to object (when processing based on legitimate interest or public interest) • Right not to be subject to solely ADM
• Provide a clear and conspicuous link on the business's homepage, titled 'Do Not Sell My Personal Information'	• No specific formatting requirements • Consent must be as easy to withdraw as it is to give

FUTURE OF PRIVACY FORUM

Right to equal service and price/'freely given consent'

CCPA: A business cannot discriminate against a consumer for exercising his or her rights	When processing is based on consent, the consent must be freely given in order for it to be valid
Businesses cannot: • Deny goods or services to the consumer • Charge different prices or rates for goods or services • Provide a different level or quality of goods or services to the consumer • Suggest that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services	• Consent is not considered freely given if the data subject has no genuine or free choice or is unable to refuse or 'withdraw consent without detriment' • The GDPR also requires that all personal data must be "processed fairly", irrespective of the lawful ground used

FUTURE OF PRIVACY FORUM

Service providers/Processors)

CCPA: A service provider is a for-profit entity that processes information on behalf of a CCPA-covered business	GDPR: A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
A 'written agreement' is required when businesses share PI with service providers for 'business purposes' (clauses not defined)	A binding contract/other legal act is required ('Article 28' agreements)
Agreement must prohibit service provider to 'retain, use, or disclose' the personal information for any purpose other than the specific business purpose included in the agreement	Content of agreement is regulated in detail by the GDPR: e.g. purpose and nature of processing, types of PD, security measures, audit rights for the controller, obligation to delete or return the data at the end of the contract
No direct obligations	Direct obligations (e.g. Art 32 - implement security measures)

What about…

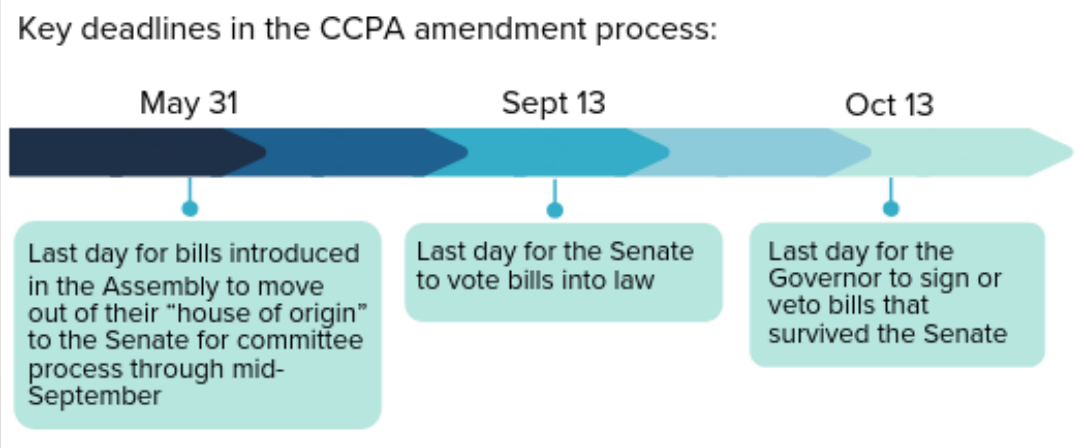
- Data protection by Design and by Default?
- Data Protection Impact Assessments?
- Data Protection Officers?
- Register of Processing Operations?

The CCPA does not include any similar accountability obligations.

FUTURE OF PRIVACY FORUM

Moving target!

CCPA can still be amended before it enters into force on January 1, 2020



Source: www.fpf.org

AND the AG of California will publish regulations, policies, procedures (which are enforceable) to detail the application of the CCPA.

FUTURE OF PRIVACY FORUM

Possible amendments to CCPA

Bill No.	Subject	Summary
AB 25	Exemption of "employee" from definition of "consumer"	– Exempts employees and contractors from the definition of "consumer."
AB 846	Loyalty programs	– Permits loyalty programs with the consumer's affirmative consent and voluntary participation; – Prohibits loyalty programs that are unjust, coercive, or unreasonable.
AB 873	Definition of personal information	– Revises definition of de-identification to include data that does not identify and is not "reasonably linkable" to a consumer; – Revises definition of personal information as being "reasonably linkable" to a consumer.
AB 874	Carve-outs from personal information	– Redefines and excludes "publicly available information" from the definition of personal information; – Clarifies that personal information does not include de-identified or aggregated data.
AB 981	Insurance transactions	– Removes consumer's right to delete or not sell personal information if it is necessary to perform an insurance transaction.

Source: www.fpf.org

AB 1146	Exemption for vehicle information	– Exempts vehicle information shared between a new auto dealer and a vehicle manufacturer when information is shared or retained pursuant to, or in anticipation of, a vehicle repair relating to warranty work or recall.
AB 1202	Data broker requirements	– Defines a "data broker" and requires data brokers to register with and provide certain information to the Attorney General, and failure to register may lead to liability (civil penalties, fees and costs).
AB 1281	Facial recognition technology: disclosure	– Requires businesses that use facial recognition technology to disclose that usage in a physical sign that is clear and conspicuous at the entrance of every location that uses facial recognition technology.
AB 1355	Addressing differential treatment and disclosures	– Under the non-discrimination provision, allows differential treatment of a consumer who has exercised CCPA rights if the differential treatment is reasonably related to value provided to the business by the consumer's information; – Requires businesses to disclose in their privacy policy consumer's right to request specific pieces of information and the categories of information collected by businesses.
AB 1416	Exceptions for businesses	– Allows an exception for businesses to: – Provide personal information to a government agency solely for the purposes of carrying out a government program; – Sell personal information of consumers who have opted-out of sale solely for the purpose of detecting security incidents, fraud or illegal activity prevention.
AB 1564	Consumer requests	– Requires businesses to make available a toll-free number, physical address, and an email address for submitting requests; – A business that exclusively operates online is only required to provide an email address for requests.

Source: www.fpf.org

Thank you!

Dr. Gabriela Zanfir-Fortuna
senior counsel
Future of Privacy Forum

Visit our site: http://www.fpf.org

Follow us!

- www.fpf.org
- @futureofprivacy
- @gabrielazanfir

FUTURE OF PRIVACY FORUM